

S **TATEMENT**
of the
American Academy
of Family Physicians

Before the

National Committee on Vital and Health Statistics
Subcommittee on Privacy and Confidentiality

Concerning

Privacy and Confidentiality in Health Care Technology

April 17, 2007

David C. Kibbe, MD MBA
Presenting

AAFP Headquarters
11400 Tomahawk Creek Parkway
Leawood, KS 66211-2672
(800) 274-2237 • (913) 906-6000
Email: fp@aafp.org



AAFP Washington Office
2021 Massachusetts Avenue, N.W.
Washington, DC 20036-1011
(202) 232-9033 Fax (202) 232-9044
Email: capitol@aafp.org

On behalf of the 93,800 members of the American Academy of Family Physicians, I am pleased to provide you with our views on the critical issues of privacy and confidentiality within a health information technology system. I am David Kibbe, MD, MBA, former Director of the Academy's Center for Health Information Technology and currently a consultant to the AAFP.

The American Academy of Family Physicians (AAFP) is one of the largest national medical organizations, representing family physicians, family medicine residents, and medical students nationwide. Founded in 1947, our mission has been to preserve and promote the science and art of family medicine and to ensure high-quality, cost-effective health care for patients of all ages.

AAFP views health information technology (HIT) systems as one way for physicians to redesign their practices so that they can coordinate patient care and provide for ongoing quality improvement at the practice level. As many of you know, the Academy has been an innovative leader in our quest to provide HIT to our members and to transform the electronic health care system as a whole.

Background

It is an opportune time for the AAFP to testify before NCVHS on privacy and confidentiality in the context of a growing debate about health information exchange and discussions regarding a so-called National Health Information Network.

Family physicians are encouraged by the growing adoption of personal health records (PHRs) by consumers and patients. Speculation also is high that electronic health records (EHRs) and EMR (electronic medical record) software applications used by AAFP members will need to interoperate with PHRs.

However, there is widespread confusion and even some apprehension about the privacy and confidentiality that will apply to these new technologies. Who owns the data? Who can access it, when, and under what restrictions or rules of confidentiality? And, specific to the subcommittee's concern, does the consumer have the right to withhold health information from his or her providers?

These are some of the issues that are commonly presented to the AAFP's Center for Health Information Technology. We believe that a lack of answers to these questions has become a significant barrier to the ongoing adoption of health information technology by our physician members. We in this country do not have a uniform set of answers to these, and many related problems.

What we *do* have is a patchwork quilt of state and federal legislation and regulatory guidance about privacy. These laws and rules are further confounded by the fact that they are industry specific and, therefore, variable with respect to the kind of personal information being considered. Unfortunately, the healthcare industry lags far behind all others: In no other industry is the issue of privacy of personal information more in need of a thorough re-visiting.

We believe that it is critical to end this confusing and unworkable situation. We need a comprehensive and uniform approach to the privacy; protection of confidentiality; and security of personal health information. Before we can address some of the specific issues, we need to fundamentally reform our approach to privacy.

Elements of a Uniform Approach to Privacy and Confidentiality

On behalf of the Academy, I would like to recommend the following four principles as a foundation on which to develop a uniform approach to privacy and confidentiality:

1. The approach should apply uniformly and consistently to any and all persons, organizations, and entities who collect, store, manage, and/or transmit health data, and not only to providers and health plans and those other entities specified under HIPAA;
2. It should allow the patient/consumer/individual to control access to the specific content of their health records, requiring that all uses to which that information might be put by the custodian or steward of the data is consented to by the individual; and
3. It should assure any limitations to that right of access and control over access, required based on the age of the information, the nature of the conditions or treatment and its relationship to issues of public health, or national security, etc., *are clearly and consistently spelled out to the individual at the time he/she provides his/her consent.*
4. It should include serious penalties, which are enforced, in the event of an illegal disclosure of private and confidential information.

The Future of Privacy

In our opinion, the HIPAA Privacy Rule is fundamentally flawed, not due to the oversight of its originators, but due to rapidly changing conditions. Most notably, this is the evolution of the Internet and the World Wide Web as vehicles for the collection, storage, management, and transfer of personal health information of many kinds, which includes health information that is personal and identifiable.

In a world in which the network also is the application, web sites and portals that offer enhancements to health content that is free to move about on the Internet already are starting to appear on the market. As you know, private companies are offering consumers web-based tools, such as personal health records that include clinical guidelines and recommendations regarding chronic illness and preventative care. This is a natural by-product of the new health data liquidity. Integrating dispersed collections of information also will become very important and drive change in the direction of personal health data management by consumers and their agents.

Traditional or legacy software applications and relational databases will remain useful in health care for a long time to come. But PHRs in the hands of consumers inevitably will boost the economic and clinical value of moving and exchanging very specific data sets and information beyond the static collections of data that providers and health plans privately format in their own databases.

Conclusion

On behalf of the AAFP, I would like to thank you for this opportunity to talk to you about the challenges we face in maintaining privacy and confidentiality in a world in which most of our key information is online. Our recommendation is that we must establish a uniform approach to privacy and confidentiality within the health care industry. We must start immediately or continue to have our outdated health care information system overtaken and overwhelmed by physicians who are unable to find a relevant privacy standard; patients who do not trust the disposition of their data; and private entities that will move in naturally to take advantage of health information opportunities.

Thank you and I would be happy to answer any questions.